

## Claims

What is claimed is:

1. A method of string extraction from biometric information comprising the steps of:  
providing a biometric information sample;  
extracting features from the biometric information sample and encoding symbols  
indicative of characteristics of the features; and,  
generating a string of the symbols indicative of the extracted features.
2. A method of string extraction from biometric information according to claim 1 wherein  
the step of extracting features from the biometric information sample comprises the step of  
identifying a feature type of an extracted feature and encoding the feature as a symbol based on  
its type.
3. A method of string extraction from biometric information according to claim 2, wherein a  
symbol is encoded as an n-bit value.
4. A method of string extraction from biometric information according to claim 2 wherein  
the step of extracting features from the biometric information sample comprises the step of  
identifying a feature location of an extracted feature and encoding the feature as a symbol based  
on its location.
5. A method of string extraction from biometric information according to claim 2 wherein  
the step of extracting features from the biometric information sample comprises the step of  
identifying a feature location of an extracted feature and encoding the feature as a symbol based  
on its orientation.

099143-072501

6. A method of string extraction from biometric information according to claim 4 wherein the step of encoding the features based on their location within the biometric information sample comprises the steps of:

providing a plurality of sectors within the biometric information sample, the sectors determined in dependence upon an identifiable and common feature within the biometric information;

determining a sector wherein a feature is located; and,

encoding a value indicative of the determined sector for the extracted feature location.

7. A method of string extraction from biometric information according to claim 6 wherein the biometric information is a fingerprint and wherein the common feature is a core of the fingerprint.

8. A method of string extraction from biometric information according to claim 1 wherein the step of generating a string of values results in an unordered string.

9. A method of string extraction from biometric information according to claim 7 wherein the step of encoding the features based on their location comprises the step of  
identifying a feature representative of the core within the biometric information sample;  
orienting the sectors relative to the identified core; and  
encoding a symbol indicative of a location of a feature other than the core relative to the core.

10. A method of string extraction from biometric information according to claim 1 further comprising the step of:

comparing the string against a previously stored string to determine a comparison value.

11. A method of string extraction from biometric information according to claim 10 further comprising the step of:

generating the previously stored string by the steps of:

0941743-072501

providing a number  $N$  of biometric information samples from a same biometric information source;

extracting a number  $r$  of features from the biometric information sample and encoding  $r$  symbols, one per feature; and,

extracting a number  $\delta$  of extra features, and encoding  $\delta$  extra symbols, one per extra feature, and

wherein the step of comparing the string includes the step of determining a number of symbols within the string that are absent from the previously stored string and deleting those symbols.

12. method of string extraction from biometric information according to claim 4 wherein the step of encoding the features based on their location within the biometric information sample further comprises the steps of:

providing a number of quantization errors tolerated;

providing a number of sector re-quantization possibilities representative of a tolerance in defining the sector quantization.

13. A method of string extraction from biometric information according to claim 12 wherein the tolerance is relative to a small rotation of the features relative to the sectors.

14. A method of string extraction from biometric information according to claim 12 wherein the tolerance is relative to a small translation of the features relative to the sectors.

15. A method of string extraction from biometric information according to claim 12 wherein the tolerance is relative to a small diagonal translation of the features relative to the sectors.

16. A method of string extraction from biometric information according to claim 1 comprising the steps of:

hashing the string of symbols to produce a of hash value for comparison with a stored hash value.

0911743 "072501  
105220" 242660

17. A method of string extraction from biometric information according to claim 16 comprising the steps of:

determining a plurality of error strings of symbols each representing a set of error features within a predetermined error range from the extracted features;

hashing strings from the plurality of error strings of symbols to produce a of hash value for comparison with the stored hash value;

comparing the hashed strings from the plurality of error strings against the stored hashed value; and,

when a hashed string and the stored hashed value are a same value, providing the error string as a password.

18. A method of string extraction from biometric information for authorizing access comprising the steps of:

providing a biometric information sample to a contact imager for imaging the biometric information sample wherein the contact imager comprises a platen disposed for accepting a biometric information source thereon;

processing the imaged information by extracting features therefrom and encoding symbols based on at least an extracted feature location within the biometric sample;

comparing a string of symbols generated from an enrollment sample and a string of symbols generated from the imaged information of the biometric sample to determine a match, wherein upon a match access is provided.

19. A method of string extraction from biometric information for authorizing access as defined in claim 18 wherein the step of comparing a string of symbols generated from an enrollment sample and a string of symbols generated from the imaged information of the biometric sample comprises the step of comparing symbols within predetermined limits wherein symbols need not match exactly.

20. A method of string extraction from biometric information for authorizing access as defined in claim 19 wherein the step of comparing symbols within predetermined limits includes the step of masking the symbols.

21. A method of string extraction from biometric information for authorizing access as defined in claim 19 wherein the step of comparing symbols within predetermined limits includes the step of comparing symbols indicative of feature locations wherein variations in symbol locations that are consistent across all symbols are not indicative of other than a match.

22. A method of string extraction from biometric information according to claim 18 wherein the step of comparing a string of symbols generated from an enrolment sample and a string of symbols generated from the imaged information of the biometric sample comprises the step of comparing symbols relating to features wherein the symbols must be indicative of a same feature type to be considered a match.

23. A method of string extraction from biometric information according to claim 18 wherein the step of extracting features therefrom and encoding symbols based on at least an extracted feature location comprises the steps of:

determining a sector wherein the extracted feature is located, the sectors disposed relative to a known feature location; and,

encoding the sector indicative of an extracted feature location.

24. A method of password generation comprising the steps of:

providing a biometric information sample;

determining from the sample a first string including a plurality of symbols, the symbols based on features within the biometric information sample;

determining a plurality of strings in dependence upon predetermined characteristics in relation to the first string;

hashing the strings from the determined plurality of strings to produce a plurality of hash values; and

0991743 072501  
T05270 E4766

comparing each hash value from the plurality of hash values against a stored hash value determined during an enrollment process for determining at least one hash string from the plurality of hash strings indicative of a match,

wherein upon a match between a hash value from the plurality of hash values and the stored hash value, the string from the plurality of strings and associated with the matching hash value is provided as the generated password.

25. A method of password generation according to claim 24 wherein the step of determining an unordered password comprises the step of:

extracting features from the biometric information sample and encoding symbols each based on at least a first extracted feature location within the biometric sample.

26. A method of password generation according to claim 24 wherein the step of determining an unordered password comprises the step of:

wherein the first extracted feature location is a core location.

27. A method of password generation according to claim 24 wherein the step of determining an unordered password comprises the step of:

wherein the first extracted feature location is a feature location for a feature selected by a biometric information source of the biometric information sample.

28. A method of password generation according to claim 24 wherein the first string is ordered based upon its symbol content.

29. A method of password generation according to claim 28 wherein the strings from the plurality of strings are ordered based upon their symbol content.

30. A method of password generation according to claim 24 wherein the step of determining a plurality of strings in dependence upon predetermined characteristics comprises the steps of:

capturing an image of a biometric information sample from a biometric information source;

extracting a number  $r$  of features from the biometric information sample and encoding  $r$  symbols, one per feature; and,

extracting a number  $\delta$  of extra features, and encoding  $\delta$  extra symbols, one per extra feature, and

wherein the step of comparing the string includes the step of determining a number of symbols within the string that are absent from the previously stored string and deleting those symbols.

31. A method of password generation according to claim 24 wherein upon the comparison of each hash value from the plurality of hash values against a stored hash value determined during an enrollment process is indicative of other than at least one hash string from the plurality of hash strings matches, verifying if the plurality of hash strings includes all the hash strings that can be generated within predetermined characteristics.

32. A method of password generation according to claim 24 wherein the generated password is an unordered generated password.

33. A method of password generation according to claim 25 wherein the step of encoding symbols is performed in dependence upon extracted feature type.

34. A method of password generation according to claim 24 wherein a symbol is encoded as an  $n$ -bit value.

35. A method of password generation comprising the steps of:  
providing a biometric information sample from an individual;  
determining a location of an alignment feature within the biometric information sample;  
extracting features from the biometric information sample;  
determining from the extracted features a first string of symbols based on locations of extracted features within the biometric information sample relative to the alignment feature;



determining a plurality of error strings in dependence upon predetermined parameters defining an error region about the extracted first string;

hashing the first string and at least some of the error strings from the determined plurality of strings to produce a plurality of hash values; and

comparing each produced hash value from the plurality of hash values with a predetermined stored hash value for determining a hash value from the plurality of hash values indicative of a match,

wherein upon a match between a hash value from the plurality of hash values and the stored hash value, the string from which the matching hash value was derived is provided as the generated password.

36. A method of password generation according to claim 35 comprising the step of: providing an indication of the first feature.

37. A method of password generation according to claim 36 wherein the step of providing an indication of the first feature includes the step of selecting the first feature from a plurality of potential first features.

38. A method of password generation according to claim 36 wherein the step of providing an indication of the first feature includes the step of selecting a region within the biometric information sample, the region being indicative of the first feature from a plurality of potential first features.

09911743-072501